FIRSTLEGAL DISCOVERY

2022

eDiscovery 101 Series

PRESENTED BY FIRST LEGAL DISCOVERY

DISCOVERY@FIRSTLEGAL.COM
WWW.FIRSTLEGALDISCOVERY.COM

eDiscovery 101 Series

The practice of law is constantly evolving, with firms expected to follow new regulations and procedures all the time. Particularly with eDiscovery, new technologies and standards of practice can make compliance a challenge and quickly lead to confusion.

Amidst this changing environment, we are seeing a trend for companies to more deeply understand their eDiscovery options. For some, it represents an opportunity to save money and put themselves in control of processes, increasing transparency and defensibility. But eDiscovery is complex, and what works for one organization might not work for another. Specific requirements will always vary by industry, a company's size, and the types of data they use.

With this increased interest in eDiscovery, we want to offer our insights into fundamentals such as information governance, legal holds, and early case assessment. But first, let's consider eDiscovery itself. It is the process each party in a case employs to preserve, collect, review, and exchange electronic information with the goal of using it as evidence. This electronically-stored information (ESI) can range from familiar data sources like emails or PDFs, to material from social media or instant messaging apps, to obscure files on a company-specific database. New data types are emerging all the time.

It is a complicated process that can involve many different departments, and largely depending on IT and Records groups. Lawyers also have their role to play; now more than ever, competency in eDiscovery is seen as part of attorneys' ethical duty to provide competent representation.

It can seem overwhelming, but thanks to modern software and eDiscovery experts there is a wide range of tools available to make things more manageable. Although ESI will only continue to become more diverse and regulations around data management will keep shifting, there will always be information available to help.

This series will explore the fundamentals of eDiscovery with the intention of educating readers on some common but complex aspects found in this important area of law practice. Among other requirements, a defensible eDiscovery process needs cooperation between both the legal and IT teams, two groups with a historically wide communication gap. This series will help to close that gap.

Throughout these white papers, we will offer information about how to build a culture of collaboration, ensure data is preserved correctly, maximize technology investments, stay up to date on current industry insights, minimize discovery-related costs, and maintain compliance with current requirements.

If you are seeking insights into the essentials of eDiscovery please join us.

Table of Contents

FIRSTLEGAL DISCOVERY

Implementing Information Governance: Maximize Data Insights and Manage Risks

EDISCOVERY 101
PART 1

DISCOVERY@FIRSTLEGAL.COM
WWW.FIRSTLEGALDISCOVERY.COM

CA PI: 24171, AZ PI: 1551710 NV LICENSE: NV PI-PS: 1452
2022

Introduction

In today's business environment, companies must produce and consume electronic data to succeed. But in recent years, there has been an explosion in the sheer amount of information that companies and employees create, collect, and store, which can carry a significant risk and cost. It's not uncommon for a company to spend disproportionate amounts of money on storing and managing unnecessary data, opening themselves up to violating the changing regulations around privacy, compliance, and security. This saturated digital landscape has given rise to the term "information governance."

[1] Peterson, Becky. "Companies Waste $62 Billion on the Cloud by Paying for Capacity They Don't Need, According to a Report." Business Insider, Business Insider, 1 Dec. 2017, https://www.businessinsider.com/companies-waste-62-billion-on-the-cloud-by-paying-for-storage-they-dont-need-according-to-a-report-2017-11.

Breaking Down Information Governance

Information governance is the foundation of the eDiscovery process. There are elements of it scattered throughout every step of eDiscovery, which is why it is critical to establish a thorough governance strategy with company data sooner rather than later.

Information governance is comprised of various policies and processes guiding the efficient use of information for an organization to realize its objectives. It is a broad term encompassing many ideas and actions that will ultimately be unique to each organization.

Nevertheless, it can be helpful to consider a definition from analyst firm Gartner[2], who explain that information governance is:

- The specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving, and deletion of information.
- The processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

It can also be useful to define data governance, which , though it is just one aspect of information governance, is a key component that most organizations will need to consider. The Data Governance Institute defines it as:[3]

- The overall management of the availability, usability, integrity, and security of the data employed in an organization or enterprise.

[2]Gartner_Inc. "Definition of Information Governance - Gartner Information Technology Glossary." Gartner, https://www.gartner.com/en/information-technology/glossary/information-governance

[3]"Definitions of Data Governance." The Data Governance Institute, 12 Sept. 2020, https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/.

Information governance is based on the standards set by records management. It begins with how data is created, stored, and eventually deleted. Note that while information governance guides the records management process, it does not replace it. The ultimate strategy is to maximize the value of any digital assets or physical information being stored, while simultaneously minimizing the risks involved with storing it.

It's also important to note that information governance is not limited to the Records and IT departments. Virtually every area of a business depends on information to function effectively, meaning that building a strategy around information governance must take the needs of every stakeholder into account. It should connect the processes, policies, metrics, and standards that are too often managed individually.

What is the goal of a successful information governance strategy? Estimates[4] claim that roughly 68% of company data being stored goes unanalyzed, essentially wasting the costs and risks associated with storing it. A successfully-implemented strategy allows a company to focus on the data that is actually valuable to them and free up server space.

Further benefits include improving[5] productivity. Harvard Business Review reports that knowledge workers can lose 50% of their time simply looking for data and trying to correct errors within it. Information governance means streamlining information access, enhancing return on investment for business intelligence systems, cutting waste, and improving analytics capabilities, among other advantages.

It's a balancing act, with concerns about the analytic use of information held against security and regulatory demands. In the end, these challenges are worthwhile when an organization is able to maximize the value of their data, stay legally compliant, and reduce discovery costs.

[4] Writer, Staff. "Two-Thirds of Data Available to Firms Goes Unused." Frontier Enterprise, 23 July 2020, https://www.frontier-enterprise.com/two-thirds-of-data-available-to-firms-goes-unused/.
[5] "Data's Credibility Problem." Harvard Business Review, 7 Oct. 2014, https://hbr.org/2013/12/datas-credibility-problem.

The Connection Between Information Governance and eDiscovery

In today's digital landscape, information is a strategic asset that must be preserved and secured with high-level coordination to ensure accountability and integrity. For information governance to be effective, companies must understand the legal and regulatory obligations with which they have to comply.

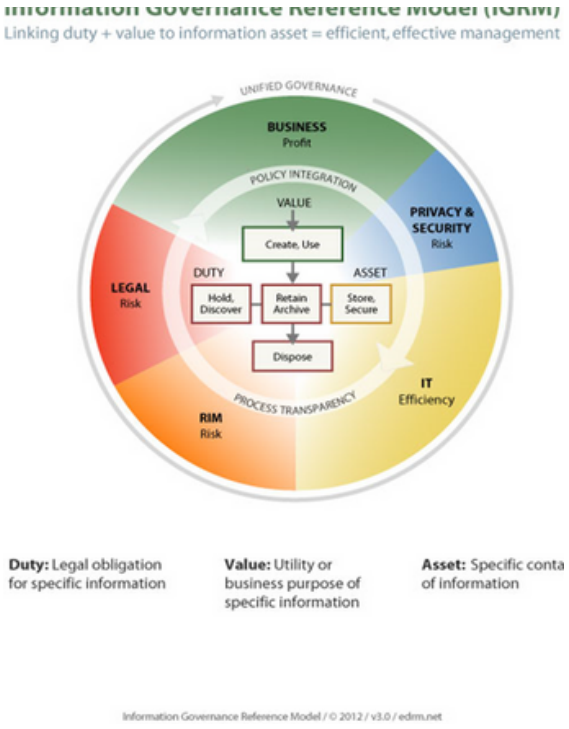
In order to identify which assets are relevant to a case, it is helpful to have a system in place for preserving, proactively de-duplicating, indexing, and searching the ESI (electronically stored information).

Since ESI is often created and stored on a variety of sources such as servers, laptops, mobile phones, hard drives, and content management systems, it can take time and specific requirements to access. However, one of the goals of an organized information governance approach is to have faster access to the precise data needed for a case or matter.

A responsible information governance system with a focus on eDiscovery needs to ask:

- How long will information be retained for?
- Who can access information, and when?
- How is sensitive information secured?
- How is all information protected from internal and external threats?

To illustrate how interdependent a successful strategy is, it can be helpful to consider EDRM's[6] information governance reference model:



The outer ring of this diagram emphasizes the interconnected structures necessary to successfully manage information. It requires not only visibility over the organization's objectives as a whole, but also knowledge of the appropriate infrastructure for information governance and awareness of any regulatory responsibilities.

Meanwhile, the center of the diagram focuses on workflow and the lifecycle of information. Significantly, disposal of information is included as a crucial piece of the puzzle, handled by both the IT department and Records & Information Management.

A recent survey[7] by EDRM and IG World Magazine found that over 90% of organizations have at least partially integrated their information governance policies with their eDiscovery programs, using the cost savings and efficiencies of eDiscovery to enhance their governance projects.

[6] "Using the IGRM Model." EDRM, 11 Feb. 2017, https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/using-the-igrm-model/.
[7] Mack, Mary, and Have you enjoyed the post ? 0 Mary Mack Mary Mack is the CEO and Chief Legal Technologist for EDRM. Mary was the co-editor of the Thomson Reuters West Treatise. "Global Information Governance Survey Results Released." EDRM, 27 Sept. 2021, https://edrm.net/2021/09/global-information-governance-survey-results-released/.

Understanding Data

Data governance is only one part of information management, but it is a critical aspect that can require very specific resources. IT-driven, it focuses on storing, transferring, and ensuring the integrity of data assets.

Maintaining data at every level of an organization and finding a robust approach to managing all assets will be an integral part of information governance and can enhance the overall strategy. Depending on the industry, leveraging digital information can lead to better insights into consumer behavior, more efficiency, and faster decision-making. Of course, there are also federal and local privacy mandates by which to abide.

Crafting a set of policies and procedures around data governance has numerous benefits, such as minimizing risks and improving data quality. It mitigates risk by systematically addressing key dangers that could compromise the organization as a result of poor data handling. Data quality is improved by creating a working environment of consistency, inclusiveness, and accuracy. Obsolete data is noted so that key decisions are not made based on it.

The process of organizing data governance often involves breaking down barriers between departments and coordinating a unified approach to data handling. This leads to improved collaboration[8] that tends to linger after the new procedures are in place. Removing these points of friction and improving camaraderie leads to more effective business.

Some[9] estimates claim that 80-90% of company information qualifies as dark data. Dark data is defined by Gartner[10] as "information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes (for example, analytics, business relationships and direct monetizing)."

It is one thing to preserve and capture data; it is another to gather appropriate insights from it. According to a survey[11] by data platform Splunk, 85% of companies are not using their dark data simply because they lack a tool to capture and analyze it.

Some form of data analytics will be integral to any information governance plan. The strategy will vary depending on the data source (for example, whether it is a text, video, image, or audio file) and typically uses artificial intelligence to gather insights.

Duties and Obligations

According to a study[12] by digital security firm Gemalto, nearly half (46%) of companies do not know where all their sensitive or private information is stored. While there is no easy way around the patchwork of privacy laws, governments still expect organizations to be compliant.

Whether it's GDPR, CCPA, or industry-specific regulations, every organization needs to be aware of their obligations when it comes to collecting and storing data such as:

- Personally identifiable information (PII)
- Personal health information (PHI)
- Payment card information

The FTC[13] requires US businesses to provide reasonable security for sensitive information. Not only are regulations updated, but the definition of personal information is subject to change. For example, in 2020 Vermont amended their data breach notification law to expand the definition of PII. In California, 2022's Genetic Information and Privacy Act limits the collection and use of PHI for direct-to-consumer genetic testing companies.

8 5 Strategies to Improve Secure Data Collaboration. https://www.snowflake.com/wp-content/uploads/2020/07/5-Strategies-to-Improve-Secure-Data-Collaboration-.pdf.
9 SethGrimes. "Unstructured Data and the 80 Percent Rule." Breakthrough Analysis, 1 Aug. 2008, https://breakthroughanalysis.com/2008/08/01/unstructured-data-and-the-80-percent-rule/.
10 Gartner_Inc. "Definition of Dark Data - Gartner Information Technology Glossary." Gartner, https://www.gartner.com/en/information-technology/glossary/dark-data.
11 "The State of Dark Data." Splunk, https://www.splunk.com/en_us/form/the-state-of-dark-data.html.
12 "Businesses Collect More Data than They Can Handle, Reveals Gemalto." Thales Group, 10 July 2018, https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/businesses-collect-more-data-than-they-can-handle-reveals-gemalto.
13 "Protecting Personal Information: A Guide for Business." Federal Trade Commission, 1 Dec. 2021, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business#Lockit.

Safely Retaining Data

A reasonable fear when retaining sensitive information is how to store it securely and limit liability in the event of a data breach. The past decade has seen harrowing examples of brands damaged and customer confidence eroded by significant data breaches, including Target, Sony, and Equifax to name but a few.

Putting an effective data retention policy into place is a significant way to minimize the risks associated with storing data. Contrary to its name, this has as much to do with responsibly disposing data as it does with keeping it. Deleted data is not at risk in a breach if it has been disposed of properly. From the perspective of legal risks, data that has been defensibly deleted does not need to be produced as part of any subsequent discovery.

Retention standards will vary by industry but once those are established, it is possible to automate the process of tracking and assessing compliance levels. Once data has been identified for disposition, it must be deleted across all media types and storage including but not limited to email, shared drives, and paper.

Good data management means accounting for every stage of the information lifecycle via strategies and policies around digital storage systems, security infrastructures, backup and protection, archiving, long-term retention, and recovery. It is an ongoing effort and organizations need to be persistent in harmonizing all of their policies governing data management.

Creating an Information Governance Strategy

After identifying who the organization's stakeholders are, the first step is conducting a thorough examination into how both digital and on-paper information is created, gathered, and stored. It's important to note how information is being used. For example, is it being shared? With whom?

From there, organizations must identify their objective and ask what key problems need to be addressed. After these questions have been answered, it is a matter of focusing on the measures that will offer solutions.

While there is no single approach that will work for all companies, some elements of successful information governance include:

ROLES AND RESPONSIBILITIES

Identifying who is on the information governance committee, the risk management team, asset management team, records management team, line managers, and employees. Anyone who plays a part in the governance strategy should have their specific responsibilities defined to avoid confusion.

DE-DUPLICATING

Maintaining a centralized catalogue where each element of information is only stored once, to avoid duplicate or abnormal versions. In this way, data is the same and authoritative for all stakeholders with proper access.

ESTABLISHED PROCEDURES

Written out and clear definitions for how information is created, shared, stored, and disposed of. These procedures might also identify associated systems that affect an organization's legal and regulatory responsibilities.

PARTNERS AND THIRD PARTIES

Those who might create, manage, or store an organization's information and need a framework establishing metrics that they are evaluated against in order to confirm compliance with overall information governance goals.

ARCHIVING DATA

A necessary component of any information governance strategy. Information can still be retrieved for compliance, litigation, or strategic requirements, but it is important to have an archival infrastructure in place as data falls out of frequent use.

ACCESS MANAGEMENT

The practice of reducing the risks triggered by unnecessary contact with data. Examine whether employees have access to data that is not required for their role, and whether that data is accessible through insecure channels. If so, limiting unnecessary access will be a component of the eventual management strategy.

COMMON TERMINOLOGY

A cohesive understanding of information that is applied uniformly across the organization. This can help prevent conflict during handoffs or inconsistent data handling policies, where different departments can sometimes get siloed into their own definitions and classification systems.

RECORDS MANAGEMENT

Crucial across any piece of information's lifecycle. It focuses on documenting the details surrounding that information, such as its identification, classification, storage, tracking, retrieval, preservation, and destruction.

DISASTER RECOVERY POLICIES

These define the procedures for reporting information losses, information breaches, incident management, and disaster recovery to improve the likelihood of retrieving lost information.

Specific information governance strategies will vary depending on the needs of each particular company, and it can be beneficial to consult professionals who have experience setting up these systems and policies.

Common Challenges

Difficulties can arise when implementing any new system, especially one as complex and expansive across departments as information governance. A successful strategy is not only about putting the right technology in place; overall buy-in from all stakeholders is an important requirement. Some common challenges include:

EXECUTIVE SUPPORT

Advocates for information governance must be prepared to educate company executives to ensure their financial and social support when it is time to enact a strategy. This might mean demonstrating the cost of unmanaged data across company resources.

OWNERSHIP

There is typically ambiguity over who should lead an organization's information governance cause, with stakeholders yielding to each other or backing out of responsibilities. Some companies have created the title of Chief Information Governance Officer as a way of addressing this.

VOLUME OF DATA

The average employee receives 120 emails[14] every day. With so much data from multiple sources being created , simply cataloguing it responsibly so it can be easily found at a later date is a monumental task.

REMOTE WORKING

Working from home was gaining popularity before the COVID-19 pandemic, and that trend is set to continue.[15] This means there exists a wider variety of devices on which ESI is being kept and created. Keeping company data accessible remotely can carry more security risks, from devices being lost or stolen to opening up remote server access.

CONFLICTING PRIORITIES

Depending on the individual stakeholder's perspective, they will seek different outcomes from successful information governance. For example, while attorneys might be concerned with mitigating risks, the IT department will need to consider data security and storage restrictions. Balancing everyone's priorities and creating an equitable system for all is an ongoing challenge of information governance.

[14] "The Surprising Reality of How Many Emails Are Sent per Day in 2022." Techjury, https://techjury.net/blog/how-many-emails-are-sent-per-day/.
[15] Lund, Susan, et al. "What's next for Remote Work: An Analysis of 2,000 Tasks, 800 Jobs, and Nine Countries." McKinsey & Company, McKinsey & Company, 3 Mar. 2021, https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries.

How to overcome these challenges? It will always depend on the organization, but there are several best practices to follow.

From the beginning, make sure every stakeholder's voice is represented. Listening to the goals, key measurables, and risk management needs of every department is essential to crafting a successful strategy. From there, doing an audit to understand what specific data the organization has is an important early step, bearing in mind that some data may not be actively managed at all, which is why it's crucial to get as complete a picture as possible.

Another best practice is to assess regulatory requirements around which data needs to be retained and for how long. These can change over time, so staying up-to-date is important as well.

With this knowledge and an audit in place, a plan for information governance can begin to take shape, prioritizing whichever data issues may be the most pressing. For example, if an initial assessment shows that the majority of data is stored in a decentralized way across a variety of devices, creating a data map connecting employees to data sources might be a priority. The exact actions to take will depend on the specific data environment.

A further predictor of successful information governance is instructing employees to execute the strategy once it is created. This training needs to be detailed so they understand how new policies and practices impact their everyday activities. Likewise, communicating why information management is important and what it has been designed to accomplish will help employees accept why changes have been put in place.

Some companies wishing to ensure compliance with new plans may introduce occasional, random audits at all levels to keep policies fresh in everyone's minds. Even without strict assessments, finding a way to measure results and review whether new strategies are working is an important element in maintaining successful information governance. Which key metrics are being tracked? What demonstrates whether the strategy has been successful? These are good questions to ask in the early planning phase so they can be built into the eventual strategy.

A Guide on Technology and Tools

It's clear that putting an information governance strategy and structure into place is a complex endeavor with many moving parts. But there are some tools that can make the prospect a little less difficult. Evaluating and implementing software options is a key component of information management.

Just as the specific approach will be unique and nuanced for each individual company, the technologies that support their strategy can vary tremendously. It's not always about utilizing a new tool, but instead about fully utilizing existing technologies and overlapping multiple systems. For example, archiving and cataloguing ESI through a content management system can help identify document owners and editors as well as creation and use dates, making searches easier and access faster. Some specific technologies to keep in mind include:

FILE ANALYSIS

A tool that examines a data vault, such as a collaborative platform server, and transmits useful information about the stored data. This can include file age, metadata, and access privileges, among other things. Utilizing this tool can make other processes more efficient, like data migration, server consolidation, and defensible disposition.

DATA MAPPING

This allows users to create, update, and organize a comprehensive directory of company data. They can help identify where specific data is kept, who has access to it, and how it is being managed. While they can be difficult to set up, there are numerous types of specialty software available to assist and once built, data maps can offer a full picture of an organization's data and its relevancy.

AUDIT LOGS

Chronological records offering evidence of the sequence of activities involved in a specific program, workflow, or event. Other software can capture and preserve these records, as well as associated data like messages, documents, or meeting records. Particularly in heavily-regulated industries, audit logs can offer crucial insights.

IN-PLACE ANALYTICS

These are designed to analyze data before collection and eDiscovery efforts begin, which is why they are also called Pre-Collection Analytics. More advanced methods include predictive coding, semantic search, and concept search.

IN-PLACE PRESERVATION

The goal of these tools is to preserve and secure ESI from being accidentally deleted by a custodian or employee prior to collection. They integrate with data sources without removing them from their original location. Even if someone intentionally deletes a file, in-place preservation technologies will keep it secure and retained with legal hold integration.

AUTOMATIC CLASSIFICATION

These systems can assign ESI to a category based on its metadata, content, or even context. Because the process is automatic, it eliminates the need to manually sort through electronic documents, saving critical resources. Once classified, ESI can be fed into automatic retrieval, archival, and disposal capabilities, depending on a company's information governance model.

ARCHIVING

These tools can keep data active should it need to be retrieved from the archives for any reason. They can manage the ingestion, location, and storage of archived information so that supervisors are able to monitor access and customize retention periods, among other capabilities.

Conclusion

Any successful information governance strategy will be an ongoing project, with regular monitoring and review needed. The nature of data and business is never going to be static, and new updates are constantly emerging. Approaches that were effective just a few years ago may no longer be in today's environment. By building these review mechanisms into their larger information governance plan, organizations can continue to improve their policies and procedures for maximum benefit.

First Legal is a litigation support company of individuals united in the common purpose of service. We are a network of experts who feel and act like an extension of our clients' team. We believe in practicing with integrity, delivering on our promises, and being personally accountable. If you are interested in establishing an information governance structure at your organization, please get in touch and we would be happy to help.

Stay tuned for Part 2! Subsequent chapter in the series will be released monthly!

WWW.FIRSTLEGALDISCOVERY.COM

DISCOVERY@FIRSTLEGAL.COM